
STANDARDS FOR SECURING REGULATED PRIVATE DATA

Date Established: May 6, 2008
Date Last Revised: June 18, 2009

Category: Information Technology
Responsible Office: Information Security Office

Summary

University at Buffalo has legal and ethical obligations to ensure that regulated private data in any form are secured in a manner that minimizes risk of unauthorized or inappropriate use or disclosure. *Regulated private data* are defined in this document as (1) Social Security number, (2) state-issued driver's license number or non-driver identification number, (3) credit or debit card number or other financial account number (4) computer access protection data such as passwords, and (5) protected health information.

Policy

POLICY STATEMENT

University Data Custodians (data owners) and Data Trustees (data access administrators) are tasked with understanding and applying the legal and ethical restrictions associated with data in their functional areas, as well as ensuring that proper procedures are in place to meet these requirements. Department managers, including Deans, Directors, Chairs, and other Managers, work with Data Trustees to ensure that their processes adhere to these data usage, handling, and security standards. All employees with access to regulated private data need to follow these security standards for handling private data.

PROTECTING THE CONFIDENTIALITY OF REGULATED PRIVATE DATA

All UB organizational units including its corporate entities must develop and follow administrative, physical, and technical procedures to protect the confidentiality of private data in any form. Standards for handling regulated private data follow.

ACCESS

Access to private data is limited to those who need to use the information in the performance of their job responsibilities. See the [Data Access and Security Policy](#) for information on the Data Trustees who grant and revoke access, as well as monitor and review access to private data.

- Steps must be taken to maintain the privacy of the data. This includes taking reasonable steps to remove private data from public view (on computer displays and paper documents), to ensure that conversations concerning the data are conducted as privately as possible, and that the data are physically secured when not in use.
- Computer systems storing private data must minimally comply with the UB Computer Password Policy.

- Strong passwords should be set on computer systems used to access sensitive data. Password screen savers, desktop locking, or logging off systems should be employed when your computer system is unattended.
- Desks and file cabinets containing private data should be locked when unattended by an individual with access to the private data.
- Laptops are inherently physically insecure since they can easily be stolen: Unencrypted private data may not be stored on laptops. Cable locks are available for securing laptop computers and act as a deterrent to theft. Special care must be taken to protect laptops against theft in airports, hotels, and other off-campus sites. (Follow [these tips](#) to protect your laptop on the road.)
- Servers containing private and regulated data should be housed in secure spaces with appropriate system access controls to protect against unauthorized access, and be protected against malicious software by following best computer security practices.
- Removable media, such as flash or jump drives, external hard drives and CD/DVDs, may not be used to store private regulated data.

USE

Private regulated data may only be used for the stated legal and/or business purpose for which the data were collected. In addition, private and regulated data may not be shared with others and may only be disclosed as authorized by law or with specific consent from the individual from whom it was collected.

- Private and regulated data may only be used in a manner consistent with authorized access and the duties and responsibilities of the position.
- Private and regulated data may not be provided to anyone without proper authorization. For example, you may not delegate your authorization/access to SSN data to anyone.
- Copies of private and regulated data or records must not be made except as required in the performance of duties.
- Private and regulated data for which there is no longer a business need must be destroyed or disposed of securely. Please see Disposal guidelines below.
- Private and regulated data must not be used for any personal or commercial purposes.
- Any suspected unauthorized access to private and regulated data must be reported immediately to the appropriate supervisor.
- Unauthorized use of private and regulated data will result in the removal of access privileges and may also result in appropriate administrative action, including, but not limited to, disciplinary and/or legal action.

TRANSMISSION

Sending private and regulated data over the Internet or by email is prohibited unless it is done in a secure environment, and steps must be taken to protect the confidentiality of fax and paper transmissions containing regulated private data.

- All electronic transactions and transmissions containing private and regulated data must either encrypt the confidential information or ensure that the connection is secure (by use of industry standard security protocols, such as ssl, ssh, sftp). Your local IT support provider

can provide information on encryption and/or using standard security protocols to transmit private and regulated data.

- All electronic transactions and transmissions must use a key length of a minimum of 128 bits.
- Interactive remote access: Private data may be accessed only through UB facilities that provide encryption, such as the campus VPN or Citrix services, and may not be accessed through third party remote desktop services, such as LogMeIn, GoToMyPC, unencrypted Windows XP Remote Desktop support service, VNC, or other desktop remote access applications.
- Private and regulated data should not be included in email text or attachments unless the data are encrypted using the FIPS 140-2 Annex A with keys stored separately except as otherwise approved by the UB Information Security Officer. Private and regulated data must be removed from paper forms and faxes unless required by law or determined to be necessary by the appropriate data trustee.
- When private and regulated data are exchanged on paper, steps must be taken so the data are not revealed. For example, the SSN must not appear in an envelope window.
- Fax transmission over telephone lines is secure if appropriate safeguards exist when faxing private and regulated data; that is, making sure the recipient's fax number is correct and the fax is not left in an unsecured area. Fax transmissions involving computer networks are not secure and should not include private and regulated data.
- When it is determined that private and regulated data must be shared with a third party, a written agreement to protect the confidentiality of the private and regulated data must be in place and the third party must agree to adhere to all UB standards and policies for securing the data.

STORAGE

Any University office that collects and maintains private and regulated data must ensure that the data are stored in a secure and confidential environment, eliminate use of the data for any purpose except that for which it was collected, and follow the guidelines below for the disposal of records containing the data. The objective is that private "data at rest", i.e., "stored private data", must be encrypted unless transmitted to a central server on a secure network vetted by the Information Security Office.

- Regulated private data may **not** be stored **unencrypted** on a University-owned local workstation or laptop. Encryption must comply with FIPS 140-2 Annex A with keys stored separately except as otherwise approved by the UB Information Security Officer. Specific permission must be obtained from the UB Information Security Officer before a user may store regulated private data on a University-owned laptop. Such permission is granted only upon demonstration of a business need and assessment of the risk of unauthorized access to or loss of the data.
- Regulated private data may **not** be copied to or stored on smart phones, floppy disks, CD/DVDs, PDAs, USB flash drives, non-University-owned/-leased computing devices, or other portable storage or computing devices. Several recent information security incidents at universities have involved the theft of such devices containing regulated private data.
- Computer applications requiring private and regulated data must store the data on a secure network server that is physically secure, i.e., protected from access by unauthorized

individuals, as well as protected against malicious software and unauthorized digital access. Encryption of the data using the FIPS 140-2 Annex A standard is advised to add another layer of security.

- On-site Storage: Tapes, disks, backups, and other electronic storage devices containing private and regulated data must reside in secure physical locations with appropriate system access controls.
- Off-site Storage: Any electronic storage media containing private and regulated data taken off-site must be protected by encryption.
- Documents and forms containing private and regulated data should be stored in a restricted access area, such as secure cabinets or a locked desk, available on a limited basis.
- Anyone working with paper documents that contain private and regulated data must take steps to protect the confidentiality of the information: desks and file cabinets containing the data should be locked when unattended.

Units must actively work to identify and remove private and regulated data from local electronic files, databases, images, and paper documents unless approval to store the data has been granted by the Information Security Officer.

DISPOSAL

Units and individuals need to comply with the following standards for the secure disposal of private data:

- Prior to recycling or disposal, desktop, laptop, and server disks containing private data must be physically destroyed or securely overwritten using the DOD 5220.22M standard for overwriting data to make it forensically unrecoverable. Your local IT support provider can provide help with this.
- Prior to disposal, steps must be taken to physically destroy or overwrite the information on portable electronic storage devices, including USB drives, disks, CD/DVDs, etc. containing private and regulated data.
- Paper documents containing private and regulated data must be shredded locally or otherwise disposed of securely.

APPLICATION ACCESS CONTROL

It is recommended that locally developed computer applications, which process private data, comply with the application development guidance described in the current [Standard Of Good Practice for Information Security](#).

Applications and systems that handle UB private data and provide a web-based interface must undergo a monthly vulnerability scan and a yearly external penetration test and periodic security audits as recommended by the Information Security Officer. Furthermore, web-servers hosting applications that handle UB private data must disable or block access to their unencrypted “HTTP” port and only make the web application available via the encrypted (“HTTPS”) port.

Access to business and systems applications must be restricted to those individuals who have a business need to access the applications or systems in the performance of their job

responsibilities. Access to source code for applications and systems must be restricted to those who have a business need for access.

COMPLIANCE

An employee or student who has substantially breached the confidentiality of regulated protected private data will be subject to disciplinary action and/or sanctions up to and including discharge and dismissal in accordance with University policy and procedures.

REPORTING OF POTENTIAL OR ACTUAL EXPOSURE OF PRIVATE DATA

Suspected or actual exposure of private data must be reported immediately to the Information Security Officer (See contacts below). All computer systems, logs and other potential evidence sources involved must be secured and retained for use in follow up investigations.

APPLICABILITY

All UB organizational units, including its corporate entities, must follow these standards.

Contact Information

Information Security Officer
CIO Office
517 Capen Hall
University at Buffalo
716-645-7979
sec-office@buffalo.edu

Related Information

University Documents:

[Protection of Private Regulated Data Policy](#)

Other Documents:

[New York State Information Security Policy](#)

Presidential Approval

Signed by President John B. Simpson

John B. Simpson, President

1/09/2009

Date